ISRAEL JOURNAL OF MATHEMATICS **167** (2008), 49–61
DOI: 10.1007/s11856-008-1040-z

NILPOTENT GROUPS ARE ROUND

BY

Daniel Berend

Departments of Mathematics and of Computer Science,
Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel
And
Department of Mathematics, Rice University,
Houston, TX 77251, USA
e-mail: berend@math.bgu.ac.il

AND

Michael D. Boshernitzan

Department of Mathematics, Rice University,
Houston, TX 77251, USA
e-mail: michael@math.rice.edu

ABSTRACT

We define a notion of roundness for finite groups. Roughly speaking, a group is round if one can order its elements in a cycle in such a way that some natural summation operators map this cycle into new cycles containing all the elements of the group. Our main result is that this combinatorial property is equivalent to nilpotence.

1. Introduction and main results

Given a finite group G of order $n = |G|$, a **cycle** in G is a finite sequence of elements of G. A cycle may be continued to a periodic sequence over G, and it will be often more convenient to think of the cycle as this sequence. A **1-1 cycle** over G is a cycle of length n, in which every element of the group appears exactly once.

Received June 12, 2006

An n-length cycle $\mathbf{g} = (g_i)_{i=0}^{n-1}$ in G is **k-round** if for every k integers $m_1, m_2, \ldots, m_k$ the cycle

$$\mathbf{g}_{m_1,m_2,\ldots,m_k} = \left(\prod_{j=1}^{k} g_{i+m_j}\right)_{i=0}^{n-1} = (g_{i+m_1} g_{i+m_2} \cdots g_{i+m_k})_{i=0}^{n-1}$$

is a 1-1 cycle in G. (The addition of indices here and later on is to be understood modulo the length n of the cycle.) Such a cycle is in particular a 1-1 cycle. (To see this, take $m_1 = m_2 = \cdots = m_k = 0$.)

The following definition plays a central role in the study initiated in this paper.

Definition 1.1: (1) G is **k-round** if it admits a k-round cycle.

(2) An n-length cycle in G is **totally round** if it is k-round for every positive integer k with $(k, n) = 1$.

(3) G is **round** if it admits a totally round cycle.

Note that G cannot possibly be k-round if $(k, n) > 1$. In fact, if p is any prime divisor of (k, n) and $\mathbf{g} = (g_i)_{i=0}^{n-1}$ is any 1-1 cycle, then the cycle $\mathbf{g}^k = (g_i^k)_{i=0}^{n-1}$ contains the identity element $1 \in G$ at least p times. This explains the constraint $(k, n) = 1$ in Definition 1.1 and Theorem 1.2 below.

Also, the property of a group being round appears to be stronger than the property of it being k-round for every k with $(k, n) = 1$. Nevertheless, the implication (2) $\Longrightarrow$ (3) in Theorem 1.2 will show that the two are in fact equivalent.

Our main result is the equivalence of the last two conditions in the following theorem.

THEOREM 1.2: *Let G be a finite group of order n. The following conditions are equivalent:*

(1) *G is k-round for some $k > n^2$;*

(2) *G is k-round for every k with $(k, n) = 1$;*

(3) *G is round;*

(4) *G is nilpotent.*

For additional equivalent conditions (for a finite group to be round), see Theorem 1.7 and Remark 1.6 below. Recall that one of the equivalent conditions

for a finite group to be nilpotent is to be isomorphic to a direct product of p-groups. (For this and other basic results used throughout the paper, we refer to any standard text, say [9].)

Theorem 1.2 implies that the family of round groups satisfies some closure properties.

COROLLARY 1.3: *Any subgroup and any quotient group of a round group is round as well.*

In a similar vein, if G is k-round and $l|k$ (l divides k), then G is l-round as well. Moreover, if $\mathbf{g}$ is a k-round cycle, then it is also l-round. In fact, let $\mathbf{g}'$ be any product of l rotates of $\mathbf{g}$. Then $\mathbf{g}'$ is obviously k/l-round, and, in particular, it is 1-1.

Example 1.4: Any finite cyclic group $\mathbf{Z}_n$ is immediately seen to be round, as the "arithmetic progression" cycle $\mathbf{g} = (i)_{i=0}^{n-1}$ is totally round. Indeed, every product $\mathbf{g}'$ of k rotates of $\mathbf{g}$ is itself an arithmetic progression whose difference is k; thus $\mathbf{g}'$ is a 1-1 cycle if $(k, n) = 1$. The fact that other finite nilpotent groups, even abelian groups such as $\mathbf{Z}_3 \times \mathbf{Z}_3$, are round is less obvious.

Remark 1.5: The first condition in Theorem 1.2, which appears weaker than the next two, may be replaced by the even weaker condition

$$G \text{ is } k\text{-round for some } k > \Phi'(n), \tag{1.1}$$

where $\Phi'(n)$ is the maximal integer which does not belong to the additive semigroup generated by the (relatively prime) numbers

$$b_i = n/p_i^{e_i} \quad 1 \le i \le r, \tag{1.2}$$

$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ being the prime power factorization of n. (This is the essence of the proof of implication (1) $\Longrightarrow$ (4) in Theorem 1.2.) Condition (1.1) indeed implies condition (1) in Theorem 1.2; see (1.3).

More generally, for a nonempty subset $S \subseteq \mathbf{N} = \{1, 2, 3, \ldots\}$ such that $\gcd(S) = 1$, denote by $\Sigma(S)$ the additive semigroup generated by S, and put $\Sigma'(S) = \mathbf{N} - \Sigma(S)$. Thus $S \subseteq \Sigma(S) \subseteq \mathbf{N}$, and $\Sigma'(S)$ is the set of positive integers which cannot be represented as finite sums of elements of S. The number

$$\Phi(S) = \sup(\Sigma'(S) \cup \{-1\})$$

is the so-called **Frobenius number** of S. It is easily seen that

$$\Phi(S) = -1 \iff 1 \in S; \quad \Phi(S) < \infty \iff \gcd(S) = 1.$$

In our case, denoting $B = \{b_i : 1 \le i \le r\}$ (see (1.2)), we observe that $\gcd(B) = 1$ and $\Phi'(n) = \Phi(B)$.

For $|S| = 2$, there exists a simple formula for the Frobenius number $\Phi(S)$, which goes back at least as far as Sylvester [16]: if $(x, y) = 1$, then $\Phi(\{x, y\}) = xy - x - y$. However, there exists no such formula for $|S| \ge 3$, nor should such a formula be expected. (See, for example, [1], [2] and the references therein for more information regarding the so-called linear diophantine problem of Frobenius.) Nevertheless, there are various upper bounds: [5],[17],[15]. Employing these bounds, we easily see that

$$\Phi'(n) = \Phi(\mathbf{B}) \le n^2. \tag{1.3}$$

(Actually, better estimates are possible for $\Phi'(n)$, but we care here about the phenomenon rather than the exact bound.)

Remark 1.6: It is possible to suggest a stronger notion of roundness. Let a cycle $\mathbf{g} = (g_i)_{i=0}^{n-1}$ over G be **strongly k-round** if for every number l of integers $m_1, m_2, \dots, m_l$ and $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_l \in \{-1, 1\}$ with $\sum_{j=1}^{l} \varepsilon_j = k$, the cycle $\left(\prod_{j=1}^{l} g_{i+m_j}^{\varepsilon_j}\right)_{i=0}^{n-1}$ is 1-1. Observe that, if $k_1 \equiv k_2 (\mathrm{mod}\, n)$, then a cycle is strongly k_1-round if and only if it is strongly k_2-round. Indeed, multiplying a product of rotates of a cycle $\mathbf{g}$ by $\mathbf{g}^n$ (or $\mathbf{g}^{-n}$) does not alter the product. We conclude that the existence of a strongly k-round cycle for some k implies the existence of such a cycle for some $k > n^2$. This cycle is, in particular, k-round, and, by Theorem 1.2, the group G is round. On the other hand, a totally round cycle is clearly strongly k-round for every k for all k relatively prime to n. Consequently, a group admits a strongly k-round cycle for some k if and only if it is round.

The above discussion is summarized in the following

THEOREM 1.7: *Let G be a finite group of order n. The following four conditions are equivalent:*

(1) *G admits a strongly 1-round cycle;*
(2) *G admits a strongly k-round cycle for some k;*
(3) *G admits a strongly k-round cycle for every k with $(k, n) = 1$;*

(4) *G is round.*

While the proof of Theorem 1.2 gives a way of constructing totally round cycles for nilpotent groups, it does not provide a way of deciding whether a given cycle is such. The following proposition gives an algorithm to that effect.

PROPOSITION 1.8: *There exists an effective constant $K = K(n)$ such that, if a 1-1 cycle $\mathbf{g}$ over a finite group G of order n is k-round for every $k \leq K$ with $(k, n) = 1$, then it is totally round.*

The following proposition demonstrates that a nonnilpotent group may still be k-round for some k's. The simplest example with $k = 2$ is given by the family of non-abelian groups whose order is a product of two distinct odd primes. Recall that, for odd primes p, q with $p < q$, a non-abelian group of order pq exists (and is unique) if and only if $q \equiv 1 (\mathrm{mod}\, p)$.

PROPOSITION 1.9: *Let G be a non-abelian group of order pq, where p, q are odd primes with $p < q$. Then G is 2-round.*

Nevertheless, some groups are **unround** — do not admit a k-round cycle for any $k > 1$. The following theorem presents two such families of groups.

THEOREM 1.10: *The following groups are unround:*

(1) *Dihedral groups of order divisible by 3.*
(2) *The symmetric group S_l for every $l \geq 3$. More generally, all sufficiently large almost simple groups with the exception of the groups ${}^2B_2(q)$ (cf.* [10]*).*

One of the motivations for this study (which is a special case of Example 1.4) was the observation that a cyclic group of odd order admits a 1-1 cycle, whose product with its rotate (by a single position) is again such.

More precisely, define an operator $\mathcal{S}$ (for sum) on the set of all cycles $\mathbf{g} = (g_i)_{i=0}^{n-1}$ over G by:

$$\mathcal{S}(\mathbf{g}) = \mathbf{g}_{0,1} = (g_i g_{i+1})_{i=0}^{n-1}, \quad \mathbf{g} \in G^n.$$

The following proposition follows in a straightforward manner from Theorem 1.2 and shows that in many cases we may apply $\mathcal{S}$ over and over again, obtaining each time a 1-1 cycle.

PROPOSITION 1.11: *A nilpotent group of odd order admits a cycle* $\mathbf{g}$ *such that* $\mathcal{S}^m(\mathbf{g})$ *is a 1-1 cycle for every positive integer* m.

In view of the above proposition, it is natural to ask whether there exists an analogue if we replace addition by subtraction. Of course, starting with a 1-1 cycle $\mathbf{g} = (g_i)_{i=0}^{n-1}$ in G, the cycle consisting of "differences" of consecutive entries of $\mathbf{g}$, namely $(g_i g_{i+1}^{-1})_{i=0}^{n-1}$, does not contain the unit element of G, and thus cannot possibly be 1-1. Thus, we shall consider now cycles of arbitrary lengths L, where $n|L$. Such a cycle is **balanced** if it contains the same number of occurrences of each element of G. Define a transformation $\mathcal{D}$ on the set of all cycles $\mathbf{g} = (g_i)_{i=0}^{L-1}$ of length L over G by

$$\mathcal{D}(\mathbf{g}) = (g_i g_{i+1}^{-1})_{i=0}^{L-1}.$$

For an integer $l \geq 1$, a cycle $\mathbf{g}$ is **$\mathcal{D}^l$-balanced** if $\mathcal{D}^r(\mathbf{g})$ is balanced for every integer $0 \leq r \leq l$. A cycle $\mathbf{g}$ is **$\mathcal{D}^\infty$-balanced** if $\mathcal{D}^r(\mathbf{g})$ is balanced for every $r \geq 1$. Finally, for $1 \leq s \leq \infty$, a group G is **$\mathcal{D}^s$-balanced** if it admits a $\mathcal{D}^s$-balanced cycle.

The following result will be shown to follow relatively easily from Theorem 1.2.

THEOREM 1.12: *Every finite nilpotent group of odd order is* $\mathcal{D}^\infty$*-balanced.*

This result should be contrasted with

THEOREM 1.13: *Every finite group is* $\mathcal{D}^r$*-balanced for all integers* $r \geq 1$.

Remark 1.14: For non-abelian groups one may consider four different versions for the transformation $\mathcal{D}$. Namely, starting from $\mathbf{g} = (g_i)_{i=0}^{L-1}$, one may let the i-th entry of $\mathcal{D}(\mathbf{g})$ be either $g_i g_{i+1}^{-1}$, as done above, or $g_{i+1}^{-1} g_i$, or $g_i^{-1} g_{i+1}$, or $g_{i+1} g_i^{-1}$. It turns out that both Theorems 1.12 and 1.13 hold for each of these variations. Moreover, the cycle $\mathbf{g}$ we construct actually has the property that we may apply at each stage any of the four variations (of the difference operator) and still get only balanced cycles.

We conjecture that the group $\mathbf{Z}_2 = \{0, 1\}$ is not $\mathcal{D}^\infty$-balanced. The conjecture would imply that no solvable finite group of even order is $\mathcal{D}^\infty$-balanced.

The authors wish to express their gratitude to V. Lev for referring them to his paper [12], which served as the initial motivation for considering the questions studied in this paper.

2. Proofs

Before proving Theorem 1.2, we present several auxiliary results.

LEMMA 2.1: *If G has a subgroup H contained in the center $Z(G) \subseteq G$, such that both H and G/H are k-round, then G is k-round as well.*

LEMMA 2.2: *If G_1 and G_2 are both k-round, then $G_1 \times G_2$ is k-round as well.*

Obviously, the following lemma contains both Lemmas 2.1 and 2.2 as special cases, so that we shall prove only it instead.

LEMMA 2.3: *If G has a normal subgroup H, each coset of which contains an element commuting with all elements of H, and if both H and G/H are k-round, then G is k-round as well.*

Remark 2.4: In fact, we prove more than is stated. Namely, the construction of a k-round cycle in G, based on such cycles in H and G/H, does not depend on k. Hence, if we start with cycles in these two groups which are k-round for several values of k, then so are the resulting cycles in G. In particular, if both H and G/H are round, then so is G.

Proof of Lemma 2.3. Let $H = \{h_0, h_1, \ldots, h_{s-1}\}$ and let $x_0, x_1, \ldots, x_{t-1}$ be representatives of all cosets of H, such that each x_j commutes with H. Rearranging the h_i's and x_j's, if necessary, we may assume that the cycle $\mathbf{h} = (h_i)_{i=0}^{s-1}$ is k-round in H and that the cycle $\mathbf{x} = (Hx_j)_{j=0}^{t-1}$ is k-round in G/H. Consider the cycle

$$\mathbf{g} = (h_0x_0, \ldots, h_0x_{t-1}, h_1x_0, \ldots, h_1x_{t-1}, \ldots, h_{s-1}x_0, \ldots, h_{s-1}x_{t-1})$$

in G. (Formally, if $0 \le i \le n-1$, write $i = at + b$ with $0 \le a \le s-1$, $0 \le b \le t-1$, and then put $g_i = h_a x_b = h_{\lfloor i/t \rfloor} x_{i \bmod t}$.) We claim that $\mathbf{g}$ is k-round. Indeed, suppose it is not. Let $m_1, m_2, \ldots, m_k$ be integers in $\{0, 1, \ldots, n-1\}$ such that

$$\prod_{j=1}^{k} g_{i+m_j} = \prod_{j=1}^{k} g_{i'+m_j} \tag{2.1}$$

for some i, i' with $0 \le i, i' \le n-1$. Projecting to G/H, we obtain

$$\prod_{j=1}^{k} Hg_{i+m_j} = \prod_{j=1}^{k} Hg_{i'+m_j},$$

that is

$$H\prod_{j=1}^{k} x_{i+m_j \,(\mathrm{mod}\, t)} = H\prod_{j=1}^{k} x_{i'+m_j \,(\mathrm{mod}\, t)}. \tag{2.2}$$

Since $\mathbf{x}$ is a k-round cycle in G/H, (2.2) implies $i \equiv i' (\mathrm{mod}\, t)$. Hence (2.1) may be rewritten in the form

$$\prod_{j=1}^{k} h_{\lfloor (i+m_j)/t \rfloor \bmod s \; x_{i+m_j \,(\mathrm{mod}\, t)}} = \prod_{j=1}^{k} h_{\lfloor (i'+m_j)/t \rfloor \bmod s \; x_{i'+m_j \,(\mathrm{mod}\, t)}}.$$

As the x_i's commute with H, this yields

$$\prod_{j=1}^{k} h_{\lfloor (i+m_j)/t \rfloor \bmod s} = \prod_{j=1}^{k} h_{\lfloor (i'+m_j)/t \rfloor \bmod s}.$$

Since $\mathbf{h}$ is a k-round cycle in H, and $i \equiv i' (\mathrm{mod}\, t)$, this implies that $\lfloor i/t \rfloor \bmod s = \lfloor i'/t \rfloor \bmod s$, and therefore $i = i'$. This proves the proposition. ∎

Our main tool for proving that a group is not k-round for a certain k is provided by the following proposition. For a finite group G and a positive integer l, denote by $R_l(G)$ the number of solutions of the equation $x^l = 1$ in G.

PROPOSITION 2.5: *Let G be a finite group of order n. If*

$$R_{l_1}(G) R_{l_2}(G) \cdots R_{l_s}(G) > n^{s-1}$$

for some positive integers $s, l_1, l_2, \ldots, l_s$, then G is not k-round for any k of the form $k = c_1 l_1 + c_2 l_2 + \cdots + c_s l_s$, where $c_1, c_2, \ldots, c_s$ are non-negative integers.

Obviously, one would usually apply the proposition with all l_i's being divisors of n and strictly positive c_i's. We may view the proposition as a strengthening of our former observation (following Definition 1.1) that G cannot be k-round if $(k, n) > 1$.

Proof. Let $\mathbf{g} = (g_i)_{i=0}^{n-1}$ be any cycle, and let k be as in the proposition. We have to show that $\mathbf{g}$ is not k-round.

Consider the cycles $\mathbf{g}^{(j)} = \mathbf{g}^{c_j l_j}$, $1 \le j \le s$. According to our assumptions, the multiplicity M_j of the identity element $1 \in G$ in $\mathbf{g}^{(j)}$ is at least $R_{l_j}(G)$. Now consider all cycles of the form $\mathbf{g}_{m_1,\ldots,m_s} = \left(\prod_{j=1}^{s} \mathbf{g}^{(j)}_{i+m_j}\right)_{i=0}^{n-1}$ as $(m_1, \ldots, m_s)$ runs through all s-tuples of integers between 0 and $n-1$. We have n^s cycles,

containing between them altogether at least $n\prod_{j=1}^{s} M_j$ occurrences of 1. Hence, at least one of these cycles contains at least

$$n\Big(\prod_{j=1}^{s} M_j\Big)/n^s \geq \Big(\prod_{j=1}^{s} R_{l_j}(G)\Big)/n^{s-1} > 1$$

occurrences of 1. Hence $\mathbf{g}$ is not k-round. ∎

In the course of the proof we shall also use the following result of Frobenius [6].

THEOREM 2.6: *Let G be a finite group of order n and let $l|n$. Then $l|R_l(G)$.*

The case where $R_l(G) = l$ is of particular interest. The following theorem, conjectured by Frobenius [6], waited almost a century for a proof.

THEOREM 2.7 ([11]): *In the setup of Theorem 2.6, if $R_l(G) = l$, then the set $\{x \in G : x^l = 1\}$ is a normal subgroup of G.*

Proof of Theorem 1.2. (2) ⇒ (1): Trivial.

(3) ⇒ (2): Trivial.

(4) ⇒ (3): Since a nilpotent group has a non-trivial center, Example 1.4, Lemma 2.1 and Remark 2.4 imply that every such group is round.

(1) ⇒ (4): Suppose G is k-round for some $k > n^2$. As explained in Remark 1.5, this implies that we may represent k in the form

$$k = n\Big(\frac{c_1}{p_1^{e_1}} + \frac{c_2}{p_2^{e_2}} + \cdots + \frac{c_r}{p_r^{e_r}}\Big)$$

for suitable positive integers $c_1, c_2, \ldots, c_r$, where

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

is the prime power factorization of n. We have to show that G is nilpotent. Consider the numbers $M_j = R_{n/p_j^{e_j}}(G)$ of solutions of the equations $x^{n/p_j^{e_j}} = 1$ in G. According to Theorem 2.6, applied with $l = n/p_j^{e_j}$, each M_j is a multiple of $n/p_j^{e_j}$, and, in particular, $M_j \geq n/p_j^{e_j}$. If for some j this inequality is strict, then $\prod_{j=1}^{r} M_j > n^{r-1}$, so that, by Proposition 2.5, G is not k-round. Thus $M_j = n/p_j^{e_j}$ for each j. According to Theorem 2.7, this implies that each of the sets

$$H_j = \{g \in G : g^{n/p_j^{e_j}} = 1\}$$

is a subgroup of G. Consider the subgroups:

$$H'_j = \bigcap_{l \neq j} H_l, \quad j = 1, 2, \ldots, r.$$

We observe that $|H'_j|\big|(n/p_l^{e_l})$ for each $l \neq j$, and therefore $|H'_j|\big|p_j^{e_j}$. On the other hand, $h \in H'_j$ if and only if $h^{p_j^{e_j}} = 1$, so that H'_j is the union of all p_j-Sylow subgroups of G.

It follows that G contains a unique p_j-Sylow subgroup for each j. Hence G is the direct product of its Sylow subgroups, which means that it is nilpotent. This completes the proof. ∎

Proof of Proposition 1.8. Take $K = (n+1)!$. Given an n-length cycle $\mathbf{g}$, which is k-round for every $k \leq K$ with $(k, n) = 1$, we have to show that it is totally round. In fact, suppose it is not totally round. Let k_0 be the minimal k with $(k, n) = 1$ for which $\mathbf{g}$ fails to be k-round. Take $m_1, m_2, \ldots, m_k$ for which $\mathbf{g}_{m_1,m_2,\ldots,m_k}$ is not 1-1. Put $k' = k_0 \bmod n$. Consider the cycles

$$\mathbf{g}_{m_1,m_2,\ldots,m_{k'}},\ \mathbf{g}_{m_1,m_2,\ldots,m_{k'+n}},\ \mathbf{g}_{m_1,m_2,\ldots,m_{k'+2n}},\ \ldots,\ \mathbf{g}_{m_1,m_2,\ldots,m_{k'+n!\cdot n}}.$$

According to our assumptions, all these are 1-1. Hence two of them are identical, say

$$\mathbf{g}_{m_1,m_2,\ldots,m_{k'+jn}} = \mathbf{g}_{m_1,m_2,\ldots,m_{k'+j'n}}.$$

It follows that

$$\mathbf{g}_{m_1,m_2,\ldots,m_k} = \mathbf{g}_{m_1,m_2,\ldots,m_{k'+jn},m_{k'+j'n+1},\ldots,m_{k_0}}.$$

The cycle on the right-hand side is a product of less than k_0 rotates of $\mathbf{g}$, and thus should be 1-1, which yields a contradiction. ∎

Proof of Proposition 1.9. We have to construct a 2-round cycle in G. Denote $r = (q-1)/p$, and let u be an integer such that

$$u \not\equiv 1 (\bmod\, q), \quad u^p \equiv 1 (\bmod\, q). \tag{2.3}$$

The group G is generated by $\{x, y\}$, satisfying the relations

$$x^q = y^p = 1,$$
$$yx = x^u y.$$

The subgroup $H = \{1, x, x^2, \ldots, x^{q-1}\}$ is normal in G. Consider the cycle

$$\mathbf{g} = (1, y, \ldots, y^{p-1}, x, xy, \ldots, xy^{p-1}, \ldots, x^{q-1}, x^{q-1}y, \ldots, x^{q-1}y^{p-1}).$$

We claim that $\mathbf{g}$ is 2-round. To this end, we have to show that, given an integer m, the cycle $\mathbf{g}_{0,m} = (g_i g_{i+m})_{i=0}^{pq-1}$ is a 1-1 cycle. Indeed, suppose

$$g_i g_{i+m} = g_{i'} g_{i'+m} \tag{2.4}$$

for some i, i' with $0 \leq i, i' \leq pq-1$. Similarly to the proof of Lemma 2.3, this can be shown to imply, since G/H is isomorphic to $\mathbf{Z}_p$, that $i \equiv i' (\mathrm{mod}\, p)$. Thus for some a_1, a_2, b_1, b_2, c we may rewrite (2.4) in the form

$$x^{a_1} y^{b_1} x^{a_2} y^{b_2} = x^{a_1+c} y^{b_1} x^{a_2+c} y^{b_2},$$

which yields (by using repeatedly the relation $yx = x^u y$ and cancelling similar terms)

$$x^{a_2 u^{b_1}} = x^{c+(a_2+c)u^{b_1}}.$$

Consequently

$$c(1 + u^{b_1}) \equiv 0 (\mathrm{mod}\, q),$$

which implies, since by (2.3) the second factor on the left-hand side cannot vanish modulo q, that $c \equiv 0 (\mathrm{mod}\, q)$. Hence, in (2.4) we have $i \equiv i' (\mathrm{mod}\, pq)$, so that $\mathbf{g}$ is indeed 2-round. ∎

Proof of Theorem 1.10. We use Proposition 2.5.

For a dihedral group D_l with $3|l$, we need to show that the group is not k-round for odd $k > 3$. Such a k may be written in the form $c \cdot 2 + 3$, and consequently the inequality

$$R_2(D_l) R_3(D_l) = (l+1) \cdot 3 > 2l = |G|$$

proves that the group is not k-round.

For an almost simple group G, other than ${}^2B_2(q)$, we have in view of [13, Section 4] and [14, Proposition 3.1, 3.2]

$$R_2(G) R_3(G) \geq c|G|^{1/2} \cdot c|G|^{3/5} > |G|$$

for an appropriate constant c. As for the dihedral group, this implies that G is not k-round for any k.

In the specific case of S_l, there is a lot of information regarding the numbers $R_j(G)$ (cf. [8] and the references therein). In particular, denoting $R_{2,l} = R_2(S_l)$, it is easy to prove the recurrence

$$R_{2,l} = R_{2,l-1} + (l-1) R_{2,l-2},$$

from which it follows [4] that $R_{2,l}/R_{2,l-1} > \sqrt{l}$, so that $R_{2,l} > \sqrt{l!}$ for $l \geq 2$. Similarly, denoting $R_{3,l} = R_3(S_l)$, it is easy to prove the recurrence

$$R_{3,l} = R_{3,l-1} + (l-1)(l-2)R_{3,l-3},$$

which implies by an easy induction that $R_{3,l} > l!^{2/3}$ for $l \geq 3$. In particular,

$$R_{2,l}R_{3,l} > l! \quad l \geq 3,$$

so that S_l, for $l \geq 3$, is not k-round for any k. ∎

Proof of Theorem 1.12. Let $(g_i)_{i=0}^{n-1}$ be a totally round cycle over G. We shall show that the $2n$-length cycle

$$\mathbf{g}' = (g_0, g_0^{-1}, g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_{n-1}, g_{n-1}^{-1})$$

is a $\mathcal{D}^\infty$-balanced cycle. In fact, it is easy to check that, for each r, the cycle $\mathcal{D}^r(\mathbf{g}')$ consists of a merge of two 1-1 cycles, as follows. The length-n cycle consisting of the entries at the places $0, 2, 4, \ldots, 2(n-1)$ is obtained by multiplying 2^r rotates of $\mathbf{g}$. The length-n cycle consisting of all other entries is obtained by inverting all entries in a product of 2^r rotates of $\mathbf{g}$. Since $\mathbf{g}$ is in particular 2^r-round, each of these subcycles is a 1-1 cycle, and therefore the whole cycle is balanced. ∎

Proof of Theorem 1.13. Let $|G| = n$. There exists a balanced cycle $\mathbf{g} = (g_i)_{i=0}^{L-1}$, with $L = n^{r+1}$, such that each of the L possible $(r+1)$-blocks of elements in G appears in $\mathbf{g}$ exactly once. (Such cycles exist; these are the so-called **complete cycles of order** $r+1$ in G, or **De Bruijn sequences** — see [3], [7, pp. 91–99]). It is straightforwardly verified that such cycles $\mathbf{g}$ must be $\mathcal{D}^r$-balanced. ∎

References

[1] J. Bak, *The linear Diophantine problem of Frobenius,* JP Journal of Algebra, Number Theory and Applications **5** (2005), 147–161.

[2] M. Beck and S. Zacks, *Refined upper bounds for the linear Diophantine problem of Frobenius,* Advances in Applied Mathematics **32** (2004), 454–467.

[3] N. G. de Bruijn, *A Combinatorial Problem,* Nederl. Acad. Wetensch. Proc. **49** (1946), 758–764; Koninklijke Nederlandse Akademie van Wetenschappen. Proceedings Indagationes Mathematicae **8** (1946), 461–467.

[4] S. Chowla, I. N. Herstein and W. Moore, *On recursions connected with symmetric groups, I,* Canadian Journal of Mathematics **3** (1951), 328–334.

[5] P. Erdős and R. L. Graham, *On a linear diophantine problem of Frobenius,* Acta Arithmetica **21** (1972), 399–408.

[6] G. Frobenius, *Verallgemeinerung des Sylowschen Satze,* Berliner Sitzungsbericht (1895), 981–993.

[7] M. Hall, Jr., *Combinatorial Theory*, John Wiley and Sons, Inc., New York, 1967.

[8] R. B. Herrera, *The number of elements of given period in finite symmetric groups,* The American Mathematical Monthly **64** (1957), 488–490.

[9] I. N. Herstein, Abstract Algebra, 3rd ed., With a preface by Barbara Cortzen and David J. Winter, Prentice Hall, Inc., Upper Saddle River, NJ, 1996.

[10] J. F. Hurley and A. Rudvalis, *Finite simple groups,* The American Mathematical Monthly **84** (1977), 693–714.

[11] N. Iiyori, *A conjecture of Frobenius and the simple groups of Lie type, IV,* Journal of Algebra **154** (1993), 188–214.

[12] V. Lev, *Permutations in abelian groups and the sequence* $n!(\mathrm{mod}\, p)$, European Journal of Combinatorics **27** (2006), 635–643.

[13] M. W. Liebeck and A. Shalev, *Classical groups, probabilistic methods, and the* $(2, 3)$*-generation problem,* Annals of Mathematics **144** (1996), 77–125.

[14] M. W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky,* Journal of Algebra **184** (1996), 31–57.

[15] E. S. Selmer, *On the linear Diophantine problem of Frobenius,* Journal f ur die Reine und Angewandte Mathematik **293/294** (1977), 1–17.

[16] J. J. Sylvester, *Mathematical questions with their solutions,* Education Times **41** (1884), 171–178.

[17] Y. Vitek, *Bounds for a linear Diophantine problem of Frobenius, II,* Canadian Journal of Mathematics **28** (1976), 1280–1288.